PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-208960
(43)Date of publication of application : 26.07.2002

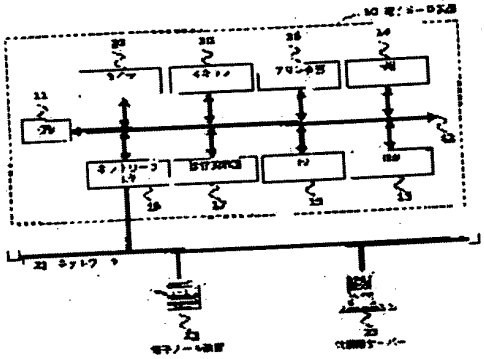
(51)Int.Cl. H04L 12/58
G09C 1/00
H04L 9/08
H04L 9/32
H04L 12/22

(21)Application number : 2001-003209
(22)Date of filing : 11.01.2001

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : MASUI TAKANORI

(54) ELECTRONIC MAIL DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To efficiently transmit a new public key to the communicating party at the time of updating the public key of its own device due to its new registration or validity expiration or the like.
SOLUTION: In this electronic mail device 10, a hard disk 15 is provided with a key pair storing means for storing a pair of keys, that is, the secret key and public key of its own device and an address information storing means for storing the address information of the electronic mail. In this case, a key pair storage detecting means for detecting that a new pair of keys are stored in the key pair storing means; and a public key transmitting means for transmitting the public key of the new pair of keys stored in the key pair storing means to the address of the electronic mail stored in the address information storing means through the electronic mail, when it is detected that the new pair of keys are stored by the key pair storage detecting means; are realized by a program to be executed by a CPU 11.



LEGAL STATUS
[Date of request for examination] 10.09.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）

公開特許公報（A）

特許出願公開番号
特開2002－208960
（Ｐ２００２－２０８９６０Ａ）
(43)公開日　平成14年７月26日(2002.7.26)

(51)Int.Cl.[7]	識別記号	FI		テーマコード（参考）
H04L 12/58	100	H04L 12/58	100 Z	5J104
G09C 1/00	640	G09C 1/00	640 Z	5K030
H04L 9/08		H04L 12/22		
9/32		9/00	601 Z	
12/22			675 D	

審査請求　未請求　請求項の数18　ＯＬ　（全14頁）

(21)出願番号　特願2001－3209(Ｐ2001－3209)

(22)出願日　平成13年１月11日(2001.1.11)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

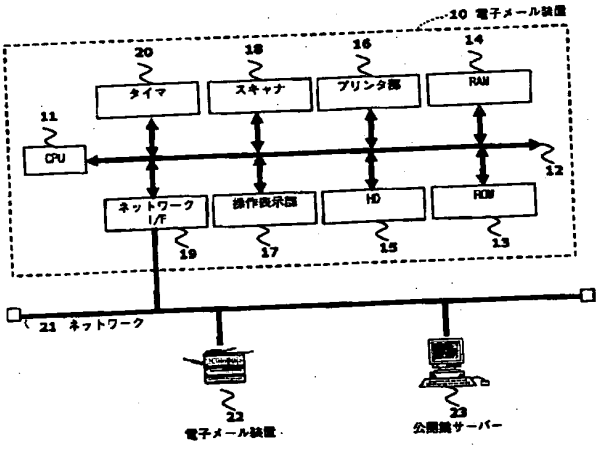
(72)発明者　益井　隆徳
神奈川県海老名市本郷2274番地　富士ゼロックス株式会社海老名事業所内

(74)代理人　100086298
弁理士　船橋　國則

Ｆターム(参考)　5J104 AA09 AA16 EA05 LA03 LA06
MA01 NA02 PA08
5K030 GA15 HA05 KA01 KA04 KA13
LD11 LD19 MB18

(54)【発明の名称】電子メール装置

(57)【要約】
【課題】　自装置の公開鍵を新規に登録または有効期限切れなどの理由により更新した場合、通信相手に効率よく新たな公開鍵を送信すること。
【解決手段】　本発明の電子メール装置１０は、自装置の秘密鍵と公開鍵との鍵ペアを記憶する鍵ペア記憶手段および電子メールのアドレス情報を記憶するアドレス情報記憶手段をハードディスク１５に備え、記鍵ペア記憶手段に新たな鍵ペアが記憶されたことを検知する鍵ペア記憶検知手段、鍵ペア記憶検知手段が新たな鍵ペアが記憶されたことを検知した場合に、鍵ペア記憶手段に記憶された新たな鍵ペアの公開鍵をアドレス情報記憶手段に記憶されている電子メールのアドレスへ電子メールで送信する公開鍵送信手段をＣＰＵ１１により実行されるプログラムで実現したものである。



1

【特許請求の範囲】

【請求項１】　公開鍵暗号方式による暗号電子メールの送受信を行う電子メール装置において、
自装置の秘密鍵と公開鍵との鍵ペアを記憶する鍵ペア記憶手段と、
前記鍵ペア記憶手段に新たな鍵ペアが記憶されたことを検知する鍵ペア記憶検知手段と、
電子メールのアドレス情報を記憶するアドレス情報記憶手段と、
前記鍵ペア記憶検知手段が新たな鍵ペアが記憶されたことを検知した場合に、前記鍵ペア記憶手段に記憶された新たな鍵ペアの公開鍵を前記アドレス情報記憶手段に記憶されている電子メールのアドレスへ電子メールで送信する公開鍵送信手段とを有することを特徴とする電子メール装置。

【請求項２】　公開鍵暗号方式による暗号電子メールの送受信を行う電子メール装置において、
自装置の秘密鍵と公開鍵との鍵ペアを記憶する鍵ペア記憶手段と、
前記鍵ペア記憶手段から鍵ペアが削除されたことを検知する鍵ペア削除検知手段と、
電子メールのアドレス情報を記憶するアドレス情報記憶手段と、
前記鍵ペア削除検知手段が前記鍵ペア記憶手段から鍵ペアが削除されたことを検知した場合に、その鍵ペアの公開鍵の削除要求を前記アドレス情報記憶手段に記憶されている電子メールのアドレスへ電子メールで送信する公開鍵削除要求送信手段とを有することを特徴とする電子メール装置。

【請求項３】　公開鍵暗号方式による暗号電子メールの送受信を行う電子メール装置において、
自装置の秘密鍵を記憶する秘密鍵記憶手段と、
前記秘密鍵に対応する公開鍵の参照アドレス情報を記憶する公開鍵参照アドレス情報記憶手段と、
前記秘密鍵記憶手段に新たな秘密鍵が記憶されたか、または前記公開鍵参照アドレス情報記憶手段に新たな公開鍵参照アドレス情報が記憶されたことを検知する記憶検知手段と、
電子メールのアドレス情報を記憶するアドレス情報記憶手段と、
前記記憶検知手段が新たな秘密鍵または新たな公開鍵参照アドレス情報が記憶されたことを検知した場合に、前記公開鍵参照アドレス情報記憶手段に記憶された公開鍵の参照アドレス情報を前記アドレス情報記憶手段に記憶されているアドレスに電子メールで送信する公開鍵参照アドレス情報送信手段とを有することを特徴とする電子メール装置。

【請求項４】　公開鍵暗号方式による暗号電子メールの送受信を行う電子メール装置において、
自装置の秘密鍵を記憶する秘密鍵記憶手段と、

2

前記秘密鍵に対応する公開鍵の参照アドレス情報を記憶する公開鍵参照アドレス情報記憶手段と、
前記秘密鍵記憶手段に新たな秘密鍵が記憶されたか、または前記公開鍵参照アドレス情報記憶手段に新たな公開鍵参照アドレス情報が記憶されたことを検知する記憶検知手段と、
電子メールのアドレス情報を記憶するアドレス情報記憶手段と、
前記記憶検知手段が新たな秘密鍵または新たな公開鍵参照アドレス情報が記憶されたことを検知した場合に、公開鍵の参照アドレス情報から公開鍵を取得する公開鍵取得手段と、
前記公開鍵取得手段が取得した公開鍵を前記アドレス情報記憶手段に記憶されているアドレスに電子メールで送信する公開鍵送信手段とを有することを特徴とする電子メール装置。

【請求項５】　請求項1または請求項４記載の電子メール装置において、
前記アドレス情報記憶手段は、電子メールのアドレス毎の暗号処理または署名処理に関する指示を示す暗号署名指示情報を有し、
前記公開鍵送信手段は、前記暗号署名指示情報において暗号処理または署名処理の実行指示があるアドレスへ公開鍵を電子メールで送信することを特徴とする電子メール装置。

【請求項６】　請求項２記載の電子メール装置において、
前記アドレス情報記憶手段は、電子メールのアドレス毎の暗号処理または署名処理に関する指示を示す暗号署名指示情報を有し、
前記公開鍵削除要求送信手段は、前記暗号署名指示情報において暗号処理または署名処理の実行指示があるアドレスへ公開鍵の削除要求を電子メールで送信することを特徴とする電子メール装置。

【請求項７】　請求項３記載の電子メール装置において、
前記アドレス情報記憶手段は、電子メールのアドレス毎の暗号処理または署名処理に関する指示を示す暗号署名指示情報を有し、
前記公開鍵参照アドレス情報送信手段は、前記暗号署名指示情報において暗号処理または署名処理の実行指示があるアドレスへ公開鍵参照アドレス情報を電子メールで送信することを特徴とする電子メール装置。

【請求項８】　請求項1または請求項４記載の電子メール装置において、
前記アドレス情報記憶手段は、電子メールのアドレス毎の公開鍵の認証者を示す認証者情報を有し、
前記公開鍵送信手段は、前記認証者情報が示す認証者が、自装置の新しい公開鍵の認証者と同じであるアドレスへ公開鍵を電子メールで送信することを特徴とする電

子メール装置。

【請求項９】　請求項２記載の電子メール装置において、

前記アドレス情報記憶手段は、電子メールのアドレス毎の公開鍵の認証者を示す認証者情報を有し、

前記公開鍵削除要求送信手段は、前記認証者情報が示す認証者が削除する公開鍵の認証者と同じであるアドレスへ公開鍵の削除要求を電子メールで送信することを特徴とする電子メール装置。

【請求項１０】　請求項３記載の電子メール装置において、

前記アドレス情報記憶手段は、電子メールのアドレス毎の公開鍵の認証者を示す認証者情報を有し、

前記公開鍵参照アドレス情報送信手段は、前記認証者情報が示す認証者が、自装置の新しい公開鍵の認証者と同じであるアドレスへ公開鍵参照アドレス情報を電子メールで送信することを特徴とする電子メール装置。

【請求項１１】　請求項1または請求項４記載の電子メール装置において、

前記アドレス情報記憶手段は、電子メールのアドレス毎の公開鍵の有無を示す公開鍵有無情報を有し、

前記公開鍵送信手段は、前記公開鍵有無情報が公開鍵が有することを示すアドレスへ公開鍵を電子メールで送信することを特徴とする電子メール装置。

【請求項１２】　請求項２記載の電子メール装置において、

前記アドレス情報記憶手段は、電子メールのアドレス毎の公開鍵の有無を示す公開鍵有無情報を有し、

前記公開鍵削除要求送信手段は、前記公開鍵有無情報が公開鍵が有することを示すアドレスへ公開鍵の削除要求を電子メールで送信することを特徴とする電子メール装置。

【請求項１３】　請求項３記載の電子メール装置において、

前記アドレス情報記憶手段は、電子メールのアドレス毎の公開鍵の有無を示す公開鍵有無情報を有し、

前記公開鍵参照アドレス情報送信手段は、前記公開鍵有無情報が公開鍵が有することを示すアドレスへ公開鍵参照アドレス情報を電子メールで送信することを特徴とする電子メール装置。

【請求項１４】　請求項1または請求項４記載の電子メール装置において、

前記アドレス情報記憶手段は、電子メールのアドレス毎の公開鍵の暗号方式を示す公開鍵暗号方式情報を有し、

前記公開鍵送信手段は、前記公開鍵暗号方式情報が示す暗号方式が、自装置の新しい公開鍵の暗号方式と同じであるアドレスへ公開鍵を電子メールで送信することを特徴とする電子メール装置。

【請求項１５】　請求項２記載の電子メール装置において、

前記アドレス情報記憶手段は、電子メールのアドレス毎の公開鍵の暗号方式を示す公開鍵暗号方式情報を有し、

前記公開鍵削除要求送信手段は、前記公開鍵暗号方式情報が示す暗号方式が削除する公開鍵の暗号方式と同じであるアドレスへ公開鍵の削除要求を電子メールで送信することを特徴とする電子メール装置。

【請求項１６】　請求項３記載の電子メール装置において、

前記アドレス情報記憶手段は、電子メールのアドレス毎の公開鍵の暗号方式を示す公開鍵暗号方式情報を有し、

前記公開鍵参照アドレス情報送信手段は、前記公開鍵暗号方式情報が示す暗号方式が、自装置の新しい公開鍵の暗号方式と同じであるアドレスへ公開鍵参照アドレス情報を電子メールで送信することを特徴とする電子メール装置。

【請求項１７】　公開鍵暗号方式による暗号電子メールの送受信を行う電子メール装置において、

電子メールを受信する受信手段と、

前記受信手段で受信した電子メールに送信者の公開鍵の参照アドレス情報が設定されていた場合に、その参照アドレス情報の示す場所から公開鍵を取得する公開鍵取得手段と、

前記公開鍵取得手段が取得した公開鍵を自装置に記憶する公開鍵記憶手段とを有することを特徴とする電子メール装置。

【請求項１８】　公開鍵暗号方式による暗号電子メールの送受信を行う電子メール装置において、

電子メールを受信する受信手段と、

前記受信手段で受信した電子メールに送信者の公開鍵の削除要求が設定されていた場合に、自装置に記憶されている送信者の公開鍵を削除する公開鍵削除手段とを有することを特徴とする電子メール装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、公開鍵暗号方式による電子署名または暗号処理を行った電子メールの送受信を行う電子メール装置に関するものであり、より詳細には、自装置に関連する公開鍵を更新した場合に、新しい公開鍵をアドレス帳に登録されている宛先に自動的に配信する電子メール装置、さらには、自装置に関連する公開鍵を失効などの理由により削除した場合に、公開鍵の削除要求をアドレス帳に登録されている宛先に自動的に配信する電子メール装置に関するものである。

【０００２】

【従来の技術】近年、電子メールを用いて、画像データをインターネット上で送受信するインターネット・ファクシミリ装置等の電子メール装置が実用化されている。このインターネット・ファクシミリ装置では、画像読み取りした原稿は、TIFF(TaggedImage File Format)形式の画像データとして電子メールに添付される。

【０００３】インターネット・ファクシミリ装置に関する技術内容は、インターネット技術の標準化組織であるIETF(Internet Engineering Task Force)が発行するRFC(Request For Comment)2301～2306に規定されている。

【０００４】ところで、電子メールは、送信元から宛先まで、インターネット上の不特定多数のメールサーバーを経由して、順次蓄積転送される。このため、インターネット上の通信路や通信経路上のメールサーバーおいて、電子メールが盗聴や改ざんされたり、あるいは、電子メールの送信者として他人になりすましされるといったセキュリティ上の脅威を有している。このため、インターネット・ファクシミリ装置などの電子メール装置を、秘匿性や非改ざん性などを要するビジネスや電子商取引の現場で利用する場合に問題となる。

【０００５】このような電子メール装置のセキュリティ上の問題を解決する方法として、従来、公開鍵暗号技術、共通鍵暗号技術やメッセージダイジェスト技術を適用した暗号電子メールが知られている。この暗号電子メールにより、電子メールの暗号化、改ざんの検知、送信者の認証が、インターネット・ファクシミリ装置などの電子メール装置で可能となる。

【０００６】例えば、暗号電子メールの技術として、MIME(Multipurpose Internet Mail Extension)機能を利用して暗号電子メールを取扱えるようにしたS/MIME(Secure MIME)やPGP/MIME(Prety Good Privacy MIME)呼ばれる技術がすでに実用されている。

【０００７】S/MIMEには、現在バージョン2とバージョン3があり、その技術内容は、それぞれIETFのRFC2311～RFC2312およびRFC2632～RFC2633に規定されている。また、PGP/MIMEの技術内容は、IETFのRFC1991,2015に規定されている。

【０００８】S/MIMEは、国際電気通信連合(ITU: International Telecommunication Union)が規定する勧告X.509の公開鍵基盤を利用しており、電子メール装置のメールアドレスと公開鍵との対応を認証局(CA: Certificate Authority)が、公開鍵証明書を発行することで保証する仕組みをとっている。

【０００９】公開鍵証明書は、認証局によって電子署名され、認証局が規定する方針によりその有効期限（通常1年）が決められている。公開鍵証明書の有効期限が経過するとその公開鍵は無効となるので、再度、新たな公開鍵と秘密鍵を生成し、新しい有効期限をもつ新たな公開鍵証明書を取得し登録する必要がある。

【００１０】PGP/MIMEの場合は、電子メール装置のメールアドレスと公開鍵との対応を認証局ではなく、他の装置であるエンティティが認証者となって保証するという仕組みを用いている。この場合も、公開鍵の所有者が設定する有効期限が切れた場合には、公開鍵を更新する必要がある。

【００１１】暗号電子メールを使って通信を行う場合、

以下の処理を行う場合には、通信相手の公開鍵が必要となる。第１は、受信した署名メールを検証する場合である。この場合、受信者は、電子メールの送信者の公開鍵を取得し、電子メールに添付されている電子署名を送信者の公開鍵で復号化して得られたダイジェスト値と電子メールの内容から計算されるダイジェスト値と比較することで正当性の検証を行う。

【００１２】第２は、電子メールを暗号化して送信する場合である。この場合は、電子メールの宛先である受信者の公開鍵を取得し、電子メールの内容の暗号化を行う対称暗号鍵をその公開鍵を使って暗号化して送信する。

【００１３】通信相手の公開鍵が有効期限切れになっていたり、または、通信相手の最新の公開鍵が取得できない場合には、上述した、受信電子メールの署名検証や電子メールの暗号化送信が処理できないという問題が発生する。

【００１４】従来、通信相手の公開鍵の取得する方法としては、通信相手から電子メールで受信した通信相手の公開鍵を自装置の公開鍵レポジトリに格納しておく方法と、認証局等が公開している外部の公開鍵サーバーから取得した通信相手の公開鍵を自装置の公開鍵レポジトリに格納しておく方法が方法がある。

【００１５】また、公開鍵を自装置の公開鍵レポジトリに格納せずに、通信の度に、外部の公開鍵サーバーから公開鍵を取得するようにすることも可能であるが、毎回サーバーへのアクセスが発生し通信のオーバーヘッドが大きいといった問題や、公開鍵サーバーへのアクセスが他人に分析され暗号送信の有無や宛先毎の暗号送信の頻度などが他人に知らやすいといった問題がある。

【００１６】通信相手の公開鍵の取得と管理に間して、特開平６－２２４８９８号公報には、相手先の公開鍵を自装置の第1ユーザー情報格納部に記憶すると共に、第２ユーザー情報格納部を設け、第1と第２のユーザー情報格納部の情報を検索することで、間違った宛先への暗号メール送信を防止する電子メール装置が開示されている。

【００１７】また、特開２０００－４９８５０号公報には、宛先の公開鍵をまず自装置の公開鍵データベースで検索し、そこで見つからない場合にのみ、外部の公開鍵サーバーから公開鍵を検索取得するオフラインでのメール送信操作が可能な電子メールの送信装置が開示されている。

【００１８】

【発明が解決しようとする課題】しかしながら、上記に説明した従来の電子メール装置では、自装置に登録されている通信相手の公開鍵の有効期限切れを検知するためには、所定の時間間隔で装置が公開鍵レポジトリに登録されている公開鍵を毎回チェックしなければならない。

【００１９】公開鍵レポジトリに登録されている通信相手の公開鍵の数が少ない場合にはさほど問題にならない

7

が、登録されている通信相手の公[redacted]の数が多くなると、公開鍵の有効期限切れ検知自体の負荷が大きくなってしまうという問題が生じる。

【００２０】また、上記に説明した従来の電子メール装置では、仮に、自分の公開鍵レポジトリに登録されている通信相手の公開鍵の有効期限切れが検知されても、HTTP(Hyper Text Transfer Protocol)プロトコルなどの公開鍵サーバーへのアクセス手段を持たない電子メール装置や公開鍵サーバーが存在しないような環境においては、通信相手の新しい公開鍵を取得するために、まず、通信相手に相手の公開鍵を電子メールで送信するよう依頼の電子メールを送信し、次に、通信相手から新しい公開鍵を電子メールで受信するといった処理が必要となる。

【００２１】この電子メールによる公開鍵送信の依頼/応答の処理は、双方の装置にかかる負荷が大きく、また、電子メールの往復処理が発生するため、公開鍵を取得するまで時間が長くなるだけでなく、相手の電子メール装置が電源OFFとなっている場合など、公開鍵を取得するまでの時間が保証できないという問題がある。

【００２２】さらに、上記に説明した従来の電子メール装置では、自装置の公開鍵を新規登録する場合や有効期限切れになどの理由で更新した場合に、その新しい公開鍵を電子メールで通信相手に配信するには、ユーザー（管理者）が通信相手を指定してメール送信を手動で行わなければならず、ユーザー（管理者）の公開鍵の配布に関わる負担が大きいという問題がある。

【００２３】また、上記に説明した従来の電子メール装置では、自装置の公開鍵を有効期限切れになどの理由で削除した場合に、通信相手は該公開鍵が無効になったことを、その公開鍵レポジトリ内に登録されている公開鍵を毎回チェックしないと、無効になったことを検知できないという問題が生じる。

【００２４】さらに、認証局が証明書廃棄リスト(CRL:Certificate Revocation List)を発行していない場合には、有効期限切れの前に、何らの理由で公開鍵を削除しても、通信相手はそれを知ることが困難であった。

【００２５】本発明は、このような問題に鑑みてなされたものであり、その目的は、自装置の公開鍵を新規登録または有効期限切れなどの理由により更新登録した場合に、当該公開鍵を使用する通信相手に当該公開鍵の更新を通知し、通信相手がその公開鍵レポジトリ内の公開鍵の有効期限切れの検査を頻繁に行うことなく、公開鍵が新たに更新されたことを容易に検知することが可能な電子メール装置を提供することにある。

【００２６】また、本発明の別の目的は、自装置の公開鍵を新規に登録または有効期限切れなどの理由により更新した場合に、該公開鍵を使用する通信相手が、公開鍵の送付依頼を送信しなくとも、自装置の新しい公開鍵を通信相手が容易に取得することが可能な電子メール装置を提供することにある。

8

【００２７】さらに、本発明の別の目的は、自装置の公開鍵を新規に登録または有効期限切れなどの理由により更新した場合に、ユーザー（管理者）が公開鍵の各宛先へ配信操作を行わなくとも、当該公開鍵を使用する通信相手に新しい当該公開鍵を自動的に配信することが可能な電子メール装置を提供することにある。

【００２８】さらに、本発明の別の目的は、自装置の公開鍵を有効期限切れなどの理由により削除した場合に、当該公開鍵を使用する通信相手がこれを検知して不要になった公開鍵を削除することが可能な電子メール装置を提供することにある。

【００２９】【課題を解決するための手段】上記目的を達成するため、請求項1記載の電子メール装置は、自装置の秘密鍵と公開鍵との鍵ペアを鍵ペア記憶手段で記憶し、頻繁に通信する相手の電子メールのアドレス情報をアドレス情報記憶手段に記憶する。鍵ペア記憶検知手段によって、鍵ペアが前記鍵ペア記憶手段に新規に記憶または更新されたことを検知すると、公開鍵送信手段が、アドレス情報記憶手段に記憶された頻繁に通信する相手の電子メールアドレスへ新たな鍵ペアの公開鍵を電子メールで送信する。これにより、通信相手が、公開鍵が更新されたことを検知可能となると共に、新しい公開鍵を取得して公開鍵レポジトリ内の公開鍵を新しい公開鍵に更新することができるようになる。

【００３０】請求項２記載の電子メール装置は、自装置の公開鍵を公開鍵記憶手段で記憶し、頻繁に通信する相手の電子メールのアドレス情報をアドレス情報記憶手段に記憶する。公開鍵削除検知手によって、公開鍵が前記公開鍵記憶手段から削除されたことを検知すると、公開鍵削除要求送信手段が、アドレス情報記憶手段に記憶された頻繁に通信する相手の電子メールアドレスへ、該公開鍵の削除要求を電子メールで送信する。これにより、通信相手が、該公開鍵が失効などの理由により削除されたことを検知可能となると共に、公開鍵を削除して公開鍵レポジトリを有効に利用することができるようになる。

【００３１】請求項３記載の電子メール装置は、自装置の秘密鍵を秘密鍵記憶手段で記憶し、その秘密鍵に対応する公開鍵が格納された公開鍵の参照アドレス情報を公開鍵参照アドレス情報記憶手段に記憶し、頻繁に通信する相手の電子メールのアドレス情報をアドレス情報記憶手段に記憶する。記憶検知手段によって、秘密鍵が前記秘密鍵記憶手段に新規に記憶または更新されたことを検知するか、または、公開鍵の参照アドレス情報が公開鍵参照アドレス情報記憶手段に新規に記憶または更新されたことを検知すると、公開鍵参照アドレス情報送信手段が、アドレス情報記憶手段に記憶された頻繁に通信する相手の電子メールアドレスへ、該公開鍵の参照アドレス

9

情報を電子メールで送信する。こ[redacted]り、通信相手が、該公開鍵が更新されたことを検知可能となると共に、新しい公開鍵の参照アドレス情報から新しい公開鍵を取得し、公開鍵レポジトリ内の公開鍵を新しい公開鍵に更新することができるようになる。

【００３２】請求項４記載の電子メール装置は、自装置の秘密鍵を秘密鍵記憶手段が記憶し、その秘密鍵に対応する公開鍵が格納された公開鍵の参照アドレス情報を公開鍵参照アドレス情報記憶手段が記憶し、頻繁に通信する相手の電子メールのアドレス情報をアドレス情報記憶手段が記憶する。記憶検知手段が、秘密鍵が前記秘密鍵記憶手段に新規に記憶または更新されたことを検知するか、または、公開鍵の参照アドレス情報が公開鍵参照アドレス情報記憶手段に新規に記憶または更新されたことを検知すると、まず、公開鍵取得手段が、該公開鍵の参照アドレス情報から公開鍵情報を取得し、次に、公開鍵参照アドレス情報送信手段が、アドレス情報記憶手段に記憶された頻繁に通信する相手の電子メールアドレスへ、取得した公開鍵を電子メールで送信する。これにより、通信相手が、該公開鍵が更新されたことを検知可能となると共に、新しい公開鍵を取得して、公開鍵レポジトリ内の公開鍵を新しい公開鍵に更新することができるようになる。

【００３３】請求項５記載の電子メール装置は、請求項1または請求項４記載の電子メール装置において、前記アドレス情報記憶手段に、宛先の電子メールのアドレス毎に、そのアドレスに対するメール送信の場合に、電子署名を行うか、暗号化を行うかの有無に関する指示情報を持ち、前記公開鍵送信手段が、電子署名を行うかあるいは暗号化を行うかのいずれかの指示が有と設定されているアドレスに対してのみ、公開鍵を送信する。これにより、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子メールアドレスのうち、暗号電子メールによる通信を行う相手にのみ、公開鍵を送信して、効率的に公開鍵を通信相手に配信することが可能となる。

【００３４】請求項６記載の電子メール装置は、請求項２記載の電子メール装置において、前記アドレス情報記憶手段に、宛先の電子メールのアドレス毎に、そのアドレスに対するメール送信の場合に、電子署名を行うか、暗号化を行うかの有無に関する指示情報を持ち、前記公開鍵削除要求送信手段が、電子署名を行うかあるいは暗号化を行うかのいずれかの指示が有と設定されているアドレスに対してのみ、公開鍵の削除要求を送信する。これにより、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子メールアドレスのうち、暗号電子メールによる通信を行う相手にのみ、公開鍵の削除要求を送信して、効率的に通信相手に公開鍵を削除させることが可能となる。

【００３５】請求項７記載の電子メール装置は、請求項３記載の電子メール装置において、前記アドレス情報記

10

憶手段に、宛先の電子メ[redacted]のアドレス毎に、そのアドレスに対するメール送信の場合に、電子署名を行うか、暗号化を行うかの有無に関する指示情報を持ち、前記公開鍵参照情報送信手段が、電子署名を行うかあるいは暗号化を行うかのいずれかの指示が有と設定されているアドレスに対してのみ、公開鍵の参照アドレス情報を送信する。これにより、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子メールアドレスのうち、暗号電子メールによる通信を行う相手にのみ、公開鍵または公開鍵の参照アドレス情報を送信して、効率的に公開鍵を通信相手に配信することが可能となる。

【００３６】請求項８記載の電子メール装置は、請求項1または請求項４記載の電子メール装置において、前記アドレス情報記憶手段に、宛先の電子メールのアドレス毎に、そのアドレスに対する公開鍵の認証者（認証局）を示す認証者情報を持ち、前記公開鍵送信手段が、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子メールアドレスのうち、自装置の新しい公開鍵の認証者と同じ公開鍵の認証者を持つ相手にのみ、公開鍵を送信する。これにより、同一の認証者による公開鍵基盤を構成している相手に効率的に公開鍵を配信することが可能となる。

【００３７】請求項９記載の電子メール装置は、請求項２記載の電子メール装置において、前記アドレス情報記憶手段に、宛先の電子メールのアドレス毎に、そのアドレスに対する公開鍵の認証者（認証局）を示す認証者情報を持ち、前記公開鍵削除要求送信手段が、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子メールアドレスのうち、削除する公開鍵の認証者と同じ公開鍵の認証者を持つ相手にのみ、公開鍵の削除要求を送信する。これにより、同一の認証者による公開鍵基盤を構成している通信相手に効率的に公開鍵を削除させることが可能となる。

【００３８】請求項１０記載の電子メール装置は、請求項３記載の電子メール装置において、前記アドレス情報記憶手段に、宛先の電子メールのアドレス毎に、そのアドレスに対する公開鍵の認証者（認証局）を示す認証者情報を持ち、前記公開鍵参照情報送信手段が、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子メールアドレスのうち、自装置の新しい公開鍵の認証者と同じ公開鍵の認証者を持つ相手にのみ、公開鍵または公開鍵の参照アドレス情報を送信する。これにより、同一の認証者による公開鍵基盤を構成している相手に効率的に公開鍵を配信することが可能となる。

【００３９】請求項１１記載の電子メール装置は、請求項1または請求項４記載の電子メール装置において、前記アドレス情報記憶手段に、宛先の電子メールのアドレス毎に、そのアドレスに対する公開鍵の有無を示す公開鍵有無情報を持ち、前記公開鍵送信手段が、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子

メールアドレスのうち、暗号電子[redacted]通信を行う公開鍵を有する相手にのみ、公開鍵を送信する。つまり、暗号電子メール通信を行わない通信相手には公開鍵を送信しないので、効率的に公開鍵を通信相手に配信することが可能となる。

【００４０】請求項１２記載の電子メール装置は、請求項２記載の電子メール装置において、前記アドレス情報記憶手段に、宛先の電子メールのアドレス毎に、そのアドレスに対する公開鍵の有無を示す公開鍵有無情報を持ち、前記公開鍵削除要求送信手段が、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子メールアドレスのうち、暗号電子メール通信を行う公開鍵を有する相手にのみ、公開鍵の削除要求を送信する。これにより、効率的に通信相手の公開鍵を削除させることが可能となる。

【００４１】請求項１３記載の電子メール装置は、請求項３記載の電子メール装置において、前記アドレス情報記憶手段に、宛先の電子メールのアドレス毎に、そのアドレスに対する公開鍵の有無を示す公開鍵有無情報を持ち、前記公開鍵参照情報送信手段が、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子メールアドレスのうち、暗号電子メール通信を行う公開鍵を有する相手にのみ、公開鍵の参照アドレス情報を送信する。つまり、暗号電子メール通信を行わない通信相手には公開鍵の参照アドレス情報を送信しないので、効率的に公開鍵を通信相手に配信することが可能となる。

【００４２】請求項１４記載の電子メール装置は、請求項1または請求項４記載の電子メール装置において、前記アドレス情報記憶手段に、宛先の電子メールのアドレス毎に、そのアドレスに対する公開鍵の暗号方式を示す公開鍵暗号方式情報を持ち、前記公開鍵送信手段が、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子メールアドレスのうち、自装置の新しい公開鍵の暗号方式と同じ公開鍵の暗号方式を持つ相手にのみ、公開鍵を送信する。つまり、公開鍵暗号方式が異なる公開鍵を持つ通信相手には公開鍵を送信しないので、同一の公開鍵暗号方式を使う相手に効率的に公開鍵を配信することが可能となる。

【００４３】請求項１５記載の電子メール装置は、請求項２記載の電子メール装置において、前記アドレス情報記憶手段に、宛先の電子メールのアドレス毎に、そのアドレスに対する公開鍵の暗号方式を示す公開鍵暗号方式情報を持ち、前記公開鍵削除要求送信手段が、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子メールアドレスのうち、削除する公開鍵の暗号方式と同じ公開鍵の暗号方式を持つ相手にのみ、公開鍵の削除要求を送信する。つまり、公開鍵暗号方式が異なる公開鍵をもつ通信相手には削除要求を送信しないので、同一の公開鍵暗号方式を使う通信相手に効率的に公開鍵を削除させることが可能となる。

【００４４】請求項１６[redacted]の電子メール装置は、請求項３記載の電子メール装置において、前記アドレス情報記憶手段に、宛先の電子メールのアドレス毎に、そのアドレスに対する公開鍵の暗号方式を示す公開鍵暗号方式情報を持ち、前記公開鍵参照情報送信手段が、アドレス情報記憶手段に記憶されている頻繁に通信する相手の電子メールアドレスのうち、自装置の新しい公開鍵の暗号方式と同じ公開鍵の暗号方式を持つ相手にのみ、公開鍵の参照アドレス情報を送信する。つまり、公開鍵暗号方式が異なる公開鍵をもつ通信相手には公開鍵の参照アドレス情報を送信することがないので、同一の公開鍵暗号方式を使う相手に効率的に公開鍵を配信することが可能となる。

【００４５】請求項１７記載の電子メール装置は、受信手段が電子メールを受信すると、受信した電子メールに送信者の公開鍵の参照アドレス情報が記述されているか否かを判定し、公開鍵の参照アドレス情報が記述さていた場合には、公開鍵取得手段がその参照アドレス情報から公開鍵を受信側で取得し、公開鍵記憶手段に記憶する。これにより、電子メールに公開鍵自体を添付して送信する場合に比べて電子メールのサイズを小さくすることができると共に、公開鍵の参照アドレスが受信された時点で公開鍵を自動的に取得しておくので、ユーザー（管理者）が操作しなくとも、自装置の公開鍵記憶手段に記憶されている公開鍵を常に最新のものにすることが可能となる。

【００４６】請求項１８記載の電子メール装置は、受信手段が電子メールを受信すると、受信した電子メールに公開鍵の削除要求が設定されているか否かを判定し、公開鍵の削除要求が設定されていた場合には、公開鍵削除手段が自装置に記憶されている送信者の公開鍵を自動的に削除する。これにより、ユーザー（管理者）が操作しなくとも、自装置の公開鍵記憶手段に記憶されている必要のない公開鍵を削除することが可能となる。

【００４７】

【発明の実施の形態】以下、本発明の実施形態について、図面を参照しながら詳細に説明する。図１は、本発明の第１および第２の実施形態に係る電子メール装置１０の概略構成とネットワーク構成を示す図である。

【００４８】図１において、１１は、ＣＰＵであり、ＲＯＭ１３に格納されたプログラムにしたがって本装置の制御を行う。１２は、アドレス・データバスであり、ＣＰＵ１１の制御対象となる各部分と接続してデータ通信を行う。１３は、ＲＯＭ（リード・オンリ・メモリ）であり電子メール装置１０の制御や電子メールの暗号や復号処理，電子メールの署名付加や署名検証処理、電子メールの送受信に関する各種プログラムが格納されている。

【００４９】ここで、各種プログラムとしては、鍵ペア記憶検知手段（自装置の秘密鍵と公開鍵との鍵ペアを記

憶する鍵ペア記憶手段に新たな鍵[redacted]記憶されたことを検知する処理を行う。）、公開鍵送信手段（新たな鍵ペアをアドレス情報記憶手段に記憶されている電子メールのアドレスへ電子メールで送信する処理を行う。）、鍵ペア削除検知手段（鍵ペア記憶手段から鍵ペアが削除されたことを検知する処理を行う。）、公開鍵削除要求送信手段（鍵ペアの公開鍵の削除要求をアドレス情報記憶手段に記憶されている電子メールのアドレスへ電子メールで送信する処理を行う。）、記憶検知手段（秘密鍵記憶手段に新たな秘密鍵が記憶されたか、または公開鍵参照アドレス情報記憶手段に新たな公開鍵参照アドレス情報が記憶されたことを検知する処理を行う。）、公開鍵参照アドレス情報送信手段（新たな公開鍵または新たな公開鍵参照アドレス情報をアドレス情報記憶手段に記憶されているアドレスに電子メールで送信する処理を行う。）、公開鍵取得手段（公開鍵の参照アドレス情報から公開鍵を取得する処理を行う。）などが挙げられる。

【００５０】１４は、ＲＡＭ（ランダム・アクセス・メモリ）でありプログラム実行時のワークメモリや電子メールの送受信の通信バッファメモリとなる。１５はハードディスク（ＨＤ）であり、受信した電子メールのデータ、自装置の秘密鍵と公開鍵証明書の鍵ペア、アドレス帳１００の各宛先のメールアドレスのデータや公開鍵証明書等や装置の各種設定パラメータの記憶保存を行う。

【００５１】本実施形態では、このハードディスク１５内に、鍵ペア記憶手段（自装置の秘密鍵と公開鍵との鍵ペアを記憶する部分）、アドレス情報記憶手段（電子メールのアドレス情報を記憶する部分）、秘密鍵記憶手段（自装置の秘密鍵を記憶する部分）、公開鍵参照アドレス情報記憶手段（秘密鍵に対応する公開鍵の参照アドレス情報を記憶する部分）を備えている。

【００５２】１６は、プリンタ部であり、受信した電子メールの本文や添付された画像ファイルの内容の印刷出力を行う。１７は、操作表示部であり、装置の状態表示やアドレス帳１００へのメールアドレスの登録操作、アドレス帳１００の各宛先毎の署名/暗号処理の有無の設定や電子メール送信指示などを行う。

【００５３】１８は、スキャナであり、電子メールに添付する原稿の画像データ読取りを行う。１９は、ネットワーク・インタフェースであり、ネットワーク３０上に接続する他の電子メール装置２１と通信を行い、電子メールの送受信を行うためのインタフェースである。

【００５４】２０は、計時を行うためのタイマである。２１は、ネットワークであり、本実施例の電子メール装置１０や本実施例の電子メール装置１０と電子メールで通信を行う他の電子メール装置２２および、認証局が管理するX.509公開鍵基盤に基づいた公開鍵証明書を記憶している公開鍵サーバー２３が接続されている。本実施形態では、X.509公開鍵基盤を利用しているが、本発明は、もちろん、これに限定されるわけでなく、PGPなどの他の公開鍵基盤を利用[redacted]もかまわない。

【００５５】図２は、本発明の第１および第２の実施形態に係る電子メール装置１０のアドレス帳１００の構成を示す図である。アドレス帳１００のデータは、宛先の電子メールアドレス１０１、公開鍵証明書の認証局１０２、公開鍵証明書ＵＲＬ(Uniform Resource Locator)１０３、公開鍵の暗号方式１０４と署名/暗号処理指示の有無１０５から構成される。

【００５６】電子メール装置１０の管理者（またはユーザー）は、操作表示部１７から頻繁に使用する宛先のメールアドレス１０１を装置のアドレス帳１００に登録する。ユーザーが電子メールを通信相手に送信する場合にはアドレス帳１００に登録されたメールアドレス１０１を参照して宛先に設定する。

【００５７】管理者（またはユーザー）は、必要に応じて、さらに、操作表示部１７から各メールアドレス毎の署名/暗号処理指示の有無１０５を設定することができる。

【００５８】メールアドレスに対応する公開鍵証明書が管理者により操作表示部１７から設定登録された場合や公開鍵証明書の添付された電子メールを受信して自動的に登録された場合には、その公開鍵証明書ＵＲＬ１０３が設定される。

【００５９】公開鍵証明書ＵＲＬ１０３において、公開鍵証明書が自装置のハードディスク１５内にある公開鍵レポジトリ（図示せず）に格納されている場合には、URLは、file://ファイル絶対パス名/となる。

【００６０】図２において、メールアドレス媒address2@domainA媒の公開鍵証明書は、URL媒file://dir/cert#01媒として記述されており、ハードディスク１５内の媒/dir媒ディレクトリの下の媒cert#01媒というファイル名で格納されていることを示している。

【００６１】また、自装置の公開鍵証明書が外部の公開鍵サーバーに格納されている場合には、URLは、アクセスプロトコル://公開鍵サーバー名/証明書ファイル名/となる。

【００６２】図２において、メールアドレス媒address3@domainB媒の公開鍵証明書は、URL媒http://server/cert#02媒として記述されており、HTTPプロトコルでアクセス可能な外部のサーバー媒server媒に媒cert#02媒というファイル名で格納されていることを示している。

【００６３】また、メールアドレスに対応する公開鍵証明書が存在する場合には、その公開鍵証明書の内容を調べて、その認証局１０２と公開鍵の暗号方式１０４が設定される。

【００６４】図２では、アドレス帳１００のメールアドレス能ochaddress2@domainA媒には、認証局CA#1に認証された公開鍵暗号方式がRSA(Rivest Shamir Adleman)方式である公開鍵証明書と、メールアドレス能ochaddress3@domainB媒には認証局CA#2に認証された公開鍵暗号方

式がDH (Diffie Hellman) 方式で[redacted]開鍵証明書が設定されている様子を示している。

【００６５】次に、本発明の第１の実施形態である電子メール装置１０において、電子メール装置１０の秘密鍵と公開鍵証明書の鍵ペアを新規または更新登録した場合および削除した場合の処理について図３、図４のフローチャートを使って説明する。なお、以下の説明で図３、図４に示されない符号は、図１、図２を参照するものとする。

【００６６】また、電子メール装置１０の秘密鍵と公開鍵証明書は、電子メール装置１０の外部のホスト装置(図示せず)で生成取得され、PKCS#12(Public Key Control Standard)フォーマットに包んで、電子メール装置１０に送信して設定するものとする。

【００６７】本発明は、もちろん、これに限定されるわけで無く、電子メール装置１０が秘密鍵と公開鍵証明書を生成取得するようにしてもよい。その場合には、電子メール装置１０は、乱数を発生することで、先ず、秘密鍵と公開鍵を生成し、そのうちの公開鍵を自分の電子メールアドレスと一緒に認証局に送付し、認証局の署名が添付された公開鍵証明書を入手することで行われる。

【００６８】電子メール装置１０は、まず、ステップＳ１０１で、登録フラグをOFFに設定する。この登録フラグは、秘密鍵と公開鍵証明書が登録されたのか削除されたのかを示すフラグである。

【００６９】次に、ステップＳ１０２で、自装置の秘密鍵と公開鍵証明書が、ハードディスク１５内の記憶部に登録されたかどうかを検知する。すでに公開鍵証明書が登録されていた場合は、すでに登録されている公開鍵証明書の有効期限が失効しておりかつ新しい公開鍵証明書の有効性が検証された場合にのみ、新しい公開鍵証明書の登録が可能となる。公開鍵証明書の有効性の検証は、公開鍵証明書の認証局の署名の有効性の検証と公開鍵証明書の有効期限の有効性により検証される。

【００７０】すでに登録されている公開鍵証明書がまだ有効であるか、新しい公開鍵証明書の有効性が検証されない場合には、新しい公開鍵証明書とそれに対応する秘密鍵は登録せずに処理を終了する。

【００７１】新しい秘密鍵と公開鍵証明書の登録が検知された場合には、ステップＳ１０３に進み、登録フラグをONに設定する。

【００７２】新しい秘密鍵と公開鍵証明書の登録が検知されない場合には、ステップＳ１０８に進み、秘密鍵と公開鍵証明書が削除されたかどうかを検知する。ここで、削除が検知されれば、ステップＳ１０４に進み、削除が検知されない場合は、本処理を終了する。

【００７３】ステップＳ１０４では、配信モードが通常配信モードであるか条件配信モードであるかの判定を行う。ここで、通常配信モードとは、アドレス帳１００に登録されている宛先のメールアドレス全てに公開鍵証明書か公開鍵削除要求を配[redacted]るモードであり、条件配信モードとは、アドレス帳１００に登録されている宛先のうち、特定の条件を満足する宛先にのみ公開鍵証明書か公開鍵証明書の削除要求を配信するモードである。この配信モードは、操作表示部１７から管理者（ユーザー）が予めいずれかの値を設定しておく。

【００７４】ステップＳ１０４において、配信モードが通常配信モードであると判定された場合には、ステップＳ１０５に進み、登録フラグがONであるかOFFであるか判定する。登録フラグがONであれば、ステップＳ１０６に進み、アドレス帳１００のメールアドレス１０１に公開鍵証明書を添付した電子メールを送信する。登録フラグがOFFであれば、ステップＳ１０９に進み、アドレス帳１００のメールアドレス１０１に公開鍵証明書の削除要求を電子メールで送信する。

【００７５】ステップＳ１０７は、アドレス帳１００に登録されている全ての宛先をチェックしたかどうかを判定するステップであり、アドレス帳１００に登録されている全ての宛先をチェックするまで、ステップＳ１０４に戻る。アドレス帳１００に登録されている全ての宛先がチェックされた場合は、本処理を終了する。

【００７６】次に、ステップＳ１０４において、配信モードが条件配信モードであると判定された場合には、ステップＳ１１０に進み、アドレス帳１００の公開鍵証明書ＵＲＬ１０３に公開鍵証明書ＵＲＬ情報が設定されているかどうかを判定する。

【００７７】公開鍵証明書ＵＲＬ１０３に公開鍵証明書ＵＲＬ情報が設定されている場合には、ステップＳ１１１に進み、アドレス帳１００のメールアドレスの認証局１０２が、ステップＳ１０２で検知した登録公開鍵証明書またはステップＳ１０８で検知した削除公開鍵証明書の認証局と同じであるかどうかを判定する。

【００７８】仮に、ステップＳ１１１で検知した公開鍵証明書の認証局が媒CA#1媒であった場合には、図２のアドレス帳１００のメールアドレス媒address2@domainA媒の公開鍵証明書の認証局媒CA#1媒が一致することになる。

【００７９】ステップＳ１１１で公開鍵証明書の認証局が同じであると判定された場合には、ステップＳ１１２に進み、さらにアドレス帳１００のメールアドレス１０１の公開鍵の暗号方式１０４が、ステップＳ１０２で検知した登録公開鍵証明書またはステップＳ１０８で検知した削除公開鍵証明書の公開鍵の暗号方式と同じであるか判定する。

【００８０】上記、ステップＳ１１０からステップＳ１１２まで全てのステップにおける判定がYESとなった場合には、ステップＳ１０５に進んで公開鍵証明書かまたは公開鍵証明書の削除要求をそのメールアドレスに送信する。

【００８１】ステップＳ１１１またはステップＳ１１２

17

のいずれかのステップにおける判[redacted]となった場合には、ステップＳ１０７に進み、そのメールアドレス１０１には公開鍵を送信せずに、次のメールアドレス１０１の判定を行う。

【００８２】ステップＳ１１０で、アドレス帳１００の公開鍵証明書URL１０３に公開鍵証明書ＵＲＬ情報が設定されていなかった場合には、ステップＳ１１１３に進み、アドレス帳１００の署名/暗号処理の指示の有無１０５を判定する。署名/暗号指示の有無１０５で署名または暗号処理のいずれかが指示されている場合には、そのメールアドレスの通信相手は公開鍵証明書を利用していると判断して、ステップＳ１０５に進んで公開鍵証明書かまたは公開鍵証明書の削除要求をそのメールアドレスに送信する。

【００８３】署名または暗号処理のすべてが指示されていない場合には、そのメールアドレスの通信相手には公開鍵証明書が不要であると判断されるので、ステップＳ１１０７に進み、そのメールアドレスには公開鍵証明書かまたは公開鍵証明書の削除要求を送信せず、次のメールアドレスの判定を行う。

【００８４】次に、本発明の第２の実施形態である電子メール装置１０の電子メールの受信処理を図５のフローチャートを使って説明する。なお、以下の説明で図５に示されない符号は図１、図２を参照するものとする。

【００８５】先ずステップＳ３０１において、電子メール装置１０が電子メールを受信すると、電子メールの内容をハードディスク１５に一次的に記憶して受信処理を実行する。

【００８６】次に、ステップＳ３０２で、受信した電子メールが送信者の公開鍵証明書の削除要求であるか判定する。受信メールが公開鍵証明書の削除要求であれば、ステップＳ３０３に進んで、その削除要求に該当する公開鍵証明書を自装置のハードディスク１５内の公開鍵レポジトリから削除する。また、受信メールが公開鍵証明書の削除要求でなければ、ステップＳ３０４に進み、電子メールの内容をプリンタ部１６から印刷出力して処理を終了する。

【００８７】次に、本発明の第２の実施形態である電子メール装置１０において、電子メール装置１０の秘密鍵と外部に登録している公開鍵証明書の参照アドレス情報を新規または更新登録した場合の処理について図６、図７のフローチャートを使って説明する。なお、以下の説明で図６、図７に示されない符号は図１、図２を参照するものとする。

【００８８】また、電子メール装置１０の秘密鍵と公開鍵証明書は、電子メール装置１０の外部のホスト装置(図示せず)で生成取得され、秘密鍵はPKCS#12(Public Key Control Standard)フォーマットに包んで、電子メール装置１０に送信して設定すると共に、認証局の公開鍵サーバー２３に格納されている公開鍵証明書ＵＲＬ情報

18

を電子メール装置１０に[redacted]するものとする。

【００８９】本発明は、もちろん、これに限定されるわけで無く、電子メール装置１０が秘密鍵と公開鍵証明書を生成取得するようにしてもよい。その場合には、電子メール装置１０は、乱数を発生することで、先ず、秘密鍵と公開鍵を生成し、そのうちの公開鍵を自分の電子メールアドレスと一緒に認証局に送付し、その認証局に認証されかつ認証局の公開鍵サーバー２３に格納されている公開鍵証明書ＵＲＬ情報を登録設定することで行われる。

【００９０】電子メール装置１０は、まず、ステップＳ２０１で、自装置の新しい秘密鍵か公開鍵証明書の参照アドレス情報（URL）が、ハードディスク１５内の記憶部に登録されたかどうかを検知する。

【００９１】すでに公開鍵証明書の参照アドレス情報（URL）が登録されていた場合は、すでに登録されている公開鍵証明書の参照アドレス情報（URL）が示す公開鍵サーバー２３に格納されている公開鍵証明書の有効期限が失効しており、かつ、新しい公開鍵証明書の参照アドレス情報（URL）が示す公開鍵サーバー２３に格納されている新しい公開鍵証明書の有効性が検証された場合にのみ、新しい公開鍵証明書の参照アドレス情報（URL）の登録が可能となる。公開鍵証明書の有効性の検証は、公開鍵証明書の認証局の署名の有効性の検証と公開鍵証明書の有効期限の有効性により検証される。

【００９２】すでに登録されている公開鍵証明書の参照アドレス情報（URL）が示す公開鍵サーバー２３に格納されている公開鍵証明書がまだ有効であるか、新しい公開鍵証明書の参照アドレス情報（URL）が示す公開鍵サーバー２３に格納されている新しい公開鍵証明書の有効性が検証されない場合には、新しい公開鍵証明書の参照アドレス情報（URL）とそれに対応する秘密鍵は登録せずに処理を終了する。

【００９３】新しい秘密鍵と公開鍵証明書の参照アドレス情報が登録された場合には、ステップＳ２０２に進み、配信モードが通常配信モードが条件配信モードであるかの判定を行う。

【００９４】ここで、通常配信モードは、アドレス帳１００に登録されている宛先のメールアドレス全てに新しい公開鍵証明書の参照アドレス情報（URL）または公開鍵証明書を配信するモードであり、条件配信モードは、アドレス帳１００に登録されている宛先のうち、特定の条件を満足する宛先にのみ新しい公開鍵証明書の参照アドレス情報（URL）または公開鍵証明書を配信するモードである。この配信モードは、操作表示部１７から管理者（ユーザー）が予め設定しておく。

【００９５】配信モードが通常配信モードである場合には、ステップＳ２０３に進み、公開鍵送信モードが、URL送信モードであるか、実体送信モードであるかの判定を行う。ここで、URL送信モードは、公開鍵証明書の参

19

照アドレス情報（URL）をメールアドレスに電子メールで送信するモードであり、実体送信モードは、公開鍵証明書をメールアドレスに電子メールで送信するモードである。ここで、この公開鍵送信モードは、操作表示部１７から管理者（ユーザー）が予め設定しておく。

【００９６】公開鍵送信モードがURL送信モードである場合には、ステップＳ２０４に進み、アドレス帳１００のメールアドレス１０１に公開鍵証明書の参照アドレス情報（URL）を電子メールに添付して送信する。

【００９７】また、公開鍵送信モードが実体送信モードである場合には、ステップＳ２０６に進み、公開鍵証明書の参照アドレス情報から、公開鍵サーバー２３に格納されている公開鍵証明書を取得し、ステップＳ２０７で、アドレス帳１００のメールアドレス１０１に取得した公開鍵証明書を電子メールに添付して送信する。

【００９８】ステップＳ２０５は、アドレス帳１００に登録されている全ての宛先をチェックしたかどうかを判定するステップであり、アドレス帳１００に登録されている全ての宛先をチェックするまで、ステップＳ２０２に戻る。アドレス帳１００に登録されている全ての宛先がチェックされた場合は、処理を終了する。

【００９９】次に、ステップＳ２０２の判定において、配信モードが条件配信モードであった場合には、ステップＳ２０８に進み、アドレス帳１００の公開鍵証明書URL１０３に公開鍵証明書ＵＲＬ情報が設定されているかどうかを判定する。

【０１００】公開鍵証明書URL１０３に公開鍵証明書ＵＲＬ情報が設定されている場合には、ステップＳ２０９に進み、アドレス帳１００のメールアドレスの認証局１０２が、ステップＳ１０で検知した新たに登録された公開鍵証明書の認証局と同じであるかどうかを判定する。

【０１０１】公開鍵証明書の認証局が同じであった場合には、ステップＳ２１０に進み、さらにアドレス帳１００のメールアドレスの公開鍵の暗号方式１０４が、新たに登録された公開鍵証明書の参照アドレス情報(URL)が示す公開鍵証明書の公開鍵の暗号方式と同じであるか判定する。

【０１０２】上記、ステップＳ２０８からステップＳ２１０まで全てのステップの判定がYESとなった場合には、ステップＳ２０３に進んで、公開鍵送信モードを判定し、判定結果に応じて公開鍵証明書の参照アドレス情報(URL)または公開鍵証明書をそのメールアドレス１０１に送信する。

【０１０３】ステップＳ２０９またはステップＳ２１０のいずれかのステップの判定でNOとなった場合には、ステップＳ２０５に進み、そのメールアドレスには公開鍵証明書の参照アドレス情報（URL）または公開鍵情報を送信せずに、アドレス帳１００内の次のメールアドレス１０１の判定を行う。

【０１０４】ステップＳ２０８で、アドレス帳１００の

20

公開鍵証明書URL１０３に公開鍵証明書ＵＲＬ情報が設定されていなかった場合には、ステップＳ２１１に進み、アドレス帳１００の署名/暗号処理の指示の有無１０５を判定する。署名/暗号指示の有無１０５で署名または暗号処理のいずれかが指示されていた場合には、そのメールアドレスの通信相手は公開鍵証明書が必要であると判断して、ステップＳ２０３に進み、公開鍵送信モードを判定し、判定結果に応じて公開鍵証明書の参照アドレス情報(URL)または公開鍵証明書をそのメールアドレス１０１に送信する。

【０１０５】署名または暗号処理のすべてが指示されていなかった場合には、そのメールアドレスの通信相手には公開鍵証明書が不要であると判断されるので、ステップＳ２０５に進み、そのメールアドレスには公開鍵証明書の参照アドレス情報（URL）または公開鍵情報を送信せずに、アドレス帳１００内の次のメールアドレス１０１の判定を行う。

【０１０６】次に、本発明の第２の実施形態である電子メール装置１０の電子メールの受信処理を図８のフローチャートを使って説明する。なお、以下の説明で図８に示されない符号は図１、図２を参照するものとする。

【０１０７】先ずステップＳ４０１において、電子メール装置１０が電子メールを受信すると、電子メールの内容をハードディスク１５に一次的に記憶して受信処理を実行する。

【０１０８】次に、ステップＳ４０２で、受信した電子メールに送信者の公開鍵証明書の参照アドレス情報（URL）が設定されているかどうかを判定する。

【０１０９】ステップＳ４０２で、受信メールに公開鍵証明書の参照アドレス情報（URL）が設定されていると判定された場合には、ステップＳ４０３に進み、その参照アドレス情報（URL）から、公開鍵証明書を取得する。

【０１１０】次に、ステップＳ４０４で、ステップＳ４０３で取得した公開鍵証明書の有効性を検証する。公開鍵証明書の有効性の検証は、公開鍵証明書の認証局の署名の有効性の検証と公開鍵証明書の有効期限の有効性により検証される。

【０１１１】次に、ステップＳ４０５で、ステップＳ４０４での有効性の検証結果をもとに公開鍵証明書が有効であるか判定する。公開鍵証明書が有効であれば、ステップＳ４０６に進み、その公開鍵証明書を自装置のハードディスク１５内の公開鍵レポジトリに登録する。

【０１１２】また、ステップＳ４０５で公開鍵証明書が無効であると判定された場合には、公開鍵証明書を登録せずに処理を終了する。

【０１１３】また、ステップＳ４０２で、受信メールに公開鍵証明書の参照アドレス情報（URL）が設定されていないと判定された場合には、ステップＳ４０７に進み、公開鍵証明書自体が添付されていないか判定を行

う。

【０１１４】ここで、公開鍵証明書自体が添付されていれば、ステップＳ４０４に進んで、公開鍵証明書の有効性検証を行い、有効であればステップＳ４０６で公開鍵証明書を自装置の公開鍵レポジトリに登録する。ここで、公開鍵証明書自体が添付されていなければ、ステップＳ４０８で、電子メールの内容をプリンタ部１６から印刷出力して処理を終了する。

【０１１５】

【発明の効果】以上説明したように、本発明の電子メール装置は、自装置の秘密鍵と公開鍵を新規登録または有効期限切れなどの理由により更新した場合に、その公開鍵を使用する通信相手に公開鍵の更新を通知するので、通信相手の公開鍵レポジトリに登録されているその公開鍵の有効期限切れを通信相手がいちいちチェックしなくとも、通信相手は自分の公開鍵レポジトリに登録されている公開鍵の有効期限切れや更新を検知することができる。

【０１１６】また、本発明の電子メール装置は、自装置の秘密鍵と公開鍵を新規登録または有効期限切れなどの理由により更新した場合に、その公開鍵を使用する通信相手が公開鍵の送信依頼を行わなくても、公開鍵または公開鍵の参照アドレス情報を自動的に配信するので、通信相手は常に新しい公開鍵を容易に入手することができるようになる。

【０１１７】さらに、本発明の電子メール装置は、自装置の秘密鍵と公開鍵を新規登録または有効期限切れなどの理由により更新した場合に、ユーザーが公開鍵の各宛先への送信操作を行わなくとも、その公開鍵を使用する通信相手に、自動的に新しい公開鍵を配信することができる。

【０１１８】さらに、本発明の電子メール装置は、自装置の公開鍵を有効期限切れなどの理由により削除した場合に、通信相手に公開鍵の削除要求を自動的に送信し、通信相手がこの削除要求を受信して不要になった公開鍵を削除するので、通信相手の公開鍵レポジトリに不要な公開鍵が登録されたままになることを防止することができる。

【図面の簡単な説明】

【図１】　本発明の実施形態における電子メール装置の概略構成とネットワーク構成を示す図である。

【図２】　本発明の実施形態における電子メール装置のアドレス帳のデータ構成を示す図である。

【図３】　本発明の第１の実施形態における電子メール装置の秘密鍵と公開鍵証明書の登録処理および削除処理の動作フローチャート（その１）である。

【図４】　本発明の第１の実施形態における電子メール装置の秘密鍵と公開鍵証明書の登録処理および削除処理の動作フローチャート（その２）である。

【図５】　本発明の第２の実施形態における電子メール装置の電子メールを受信処理の動作フローチャートである。

【図６】　本発明の第２の実施形態における電子メール装置の秘密鍵と公開鍵証明書の参照アドレス情報（URL）の登録処理の動作フローチャート（その１）である。

【図７】　本発明の第２の実施形態における電子メール装置の秘密鍵と公開鍵証明書の参照アドレス情報（URL）の登録処理の動作フローチャート（その２）である。

【図８】　本発明の第２の実施形態における電子メール装置の電子メールの受信処理の動作フローチャートである。

【符号の説明】

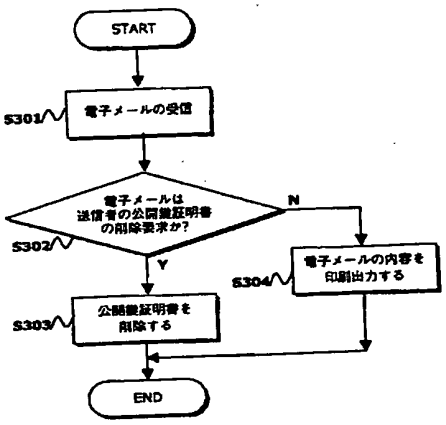
１０，２２…電子メール装置、１１…ＣＰＵ、１２…アドレス・データバス、１３…ＲＯＭ（リード・オンリ・メモリ）、１４…ＲＡＭ（ランダム・アクセス・メモリ）、１５…ハードディスク、１６…プリンタ部、１７…操作表示部、１８…スキャナ、１９…ネットワーク・インタフェース、２０…タイマ、２３…公開鍵サーバー

【図２】

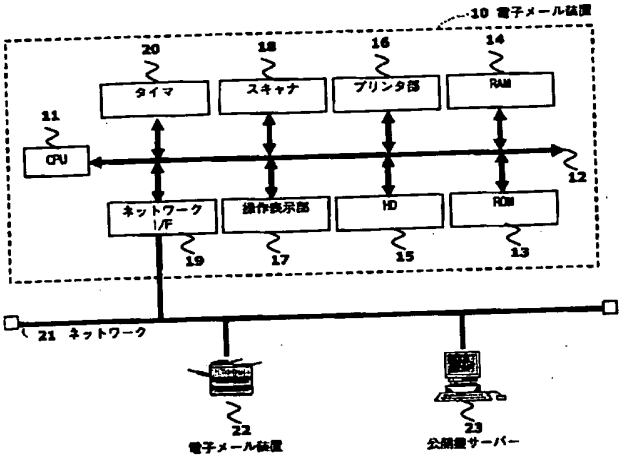
100 アドレス帳

101 メールアドレス	102 認証局	103 公開鍵証明書 URL	104 暗号方式	105 署名/暗号
address1@domainA	設定なし	なし	設定なし	設定なし
address2@domainA	CA#1	file://dir/cert#01	RSA	署名+暗号
address3@domainB	CA#2	http://server/cert#02	DH	暗号

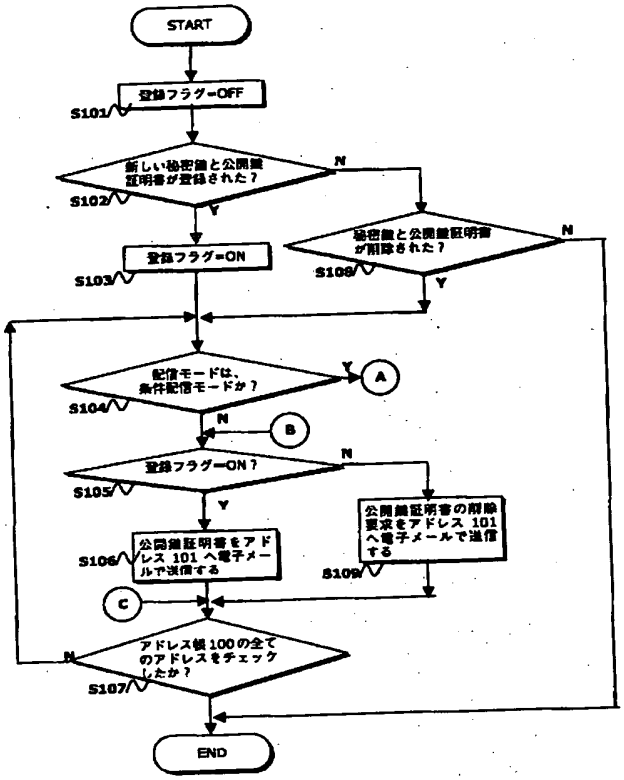
【図５】



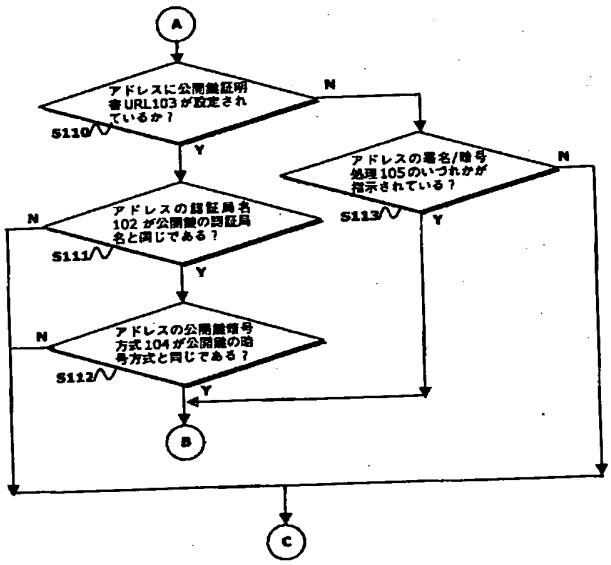
【図１】


10 電子メール装置
20
タイマ
18
スキャナ
16
プリンタ部
14
RAM
11
CPU
12
ネットワーク I/F
19
操作表示部
17
HD
15
ROM
13
21 ネットワーク
22
電子メール装置
23
公開鍵サーバー

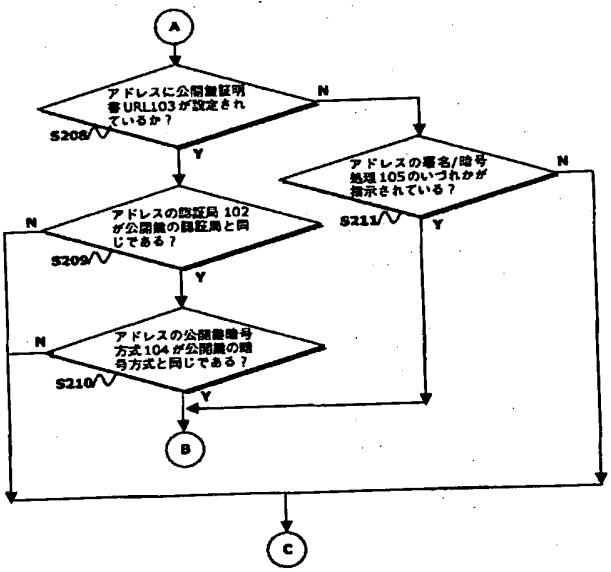
【図３】


START
登録フラグ=OFF
S101
新しい秘密鍵と公開鍵証明書が登録された？
S102
N
Y
登録フラグ=ON
S103
秘密鍵と公開鍵証明書が削除された？
S108
N
Y
配信モードは、条件配信モードか？
S104
Y
A
N
B
登録フラグ=ON？
S105
N
Y
公開鍵証明書をアドレス 101 へ電子メールで送信する
S106
公開鍵証明書の削除要求をアドレス 101 へ電子メールで送信する
S109
C
アドレス帳 100 の全てのアドレスをチェックしたか？
S107
N
END

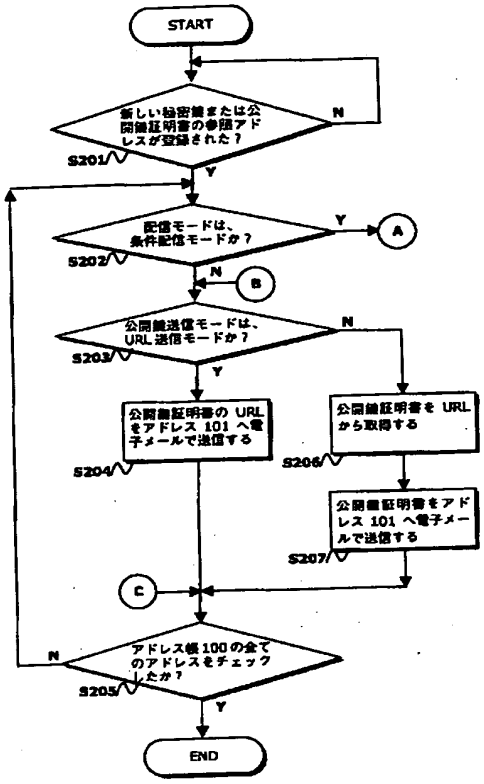
【図４】


A
アドレスに公開鍵証明書 URL103 が設定されているか？
S110
N
Y
アドレスの署名/暗号処理 105 のいづれかが指示されている？
S113
N
Y
アドレスの認証局名 102 が公開鍵の認証局名と同じである？
S111
N
Y
アドレスの公開鍵暗号方式 104 が公開鍵の暗号方式と同じである？
S112
N
Y
B
C

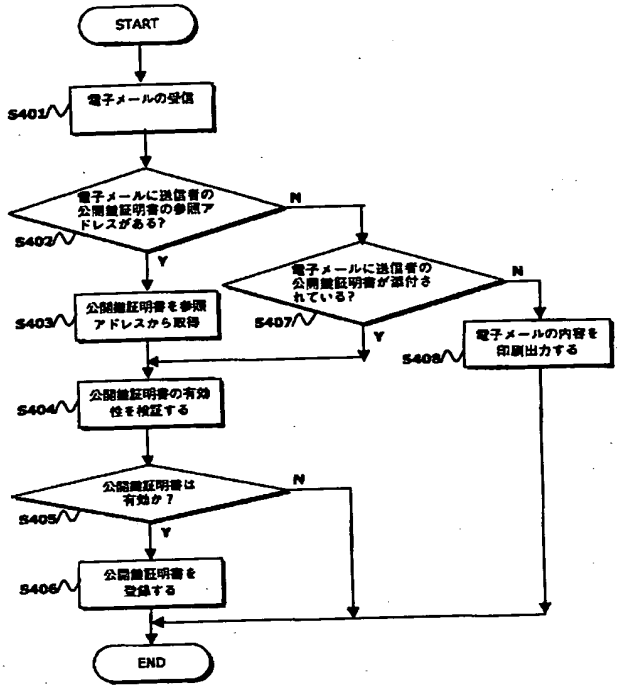
【図７】


A
アドレスに公開鍵証明書 URL103 が設定されているか？
S208
N
Y
アドレスの署名/暗号処理 105 のいづれかが指示されている？
S211
N
Y
アドレスの認証局 102 が公開鍵の認証局と同じである？
S209
N
Y
アドレスの公開鍵暗号方式 104 が公開鍵の暗号方式と同じである？
S210
N
Y
B
C

【図６】


START
新しい秘密鍵または公開鍵証明書の参照アドレスが登録された？
S201
N
Y
配信モードは、条件配信モードか？
S202
Y
A
N
B
公開鍵送信モードは、URL送信モードか？
S203
N
Y
公開鍵証明書の URL をアドレス 101 へ電子メールで送信する
S204
公開鍵証明書を URL から取得する
S206
公開鍵証明書をアドレス 101 へ電子メールで送信する
S207
C
アドレス帳100の全てのアドレスをチェックしたか？
S205
N
Y
END

【図８】


START
電子メールの受信
S401
電子メールに送信者の公開鍵証明書の参照アドレスがある？
S402
N
Y
電子メールに送信者の公開鍵証明書が添付されている？
S407
N
Y
電子メールの内容を印刷出力する
S408
公開鍵証明書を参照アドレスから取得
S403
公開鍵証明書の有効性を検証する
S404
公開鍵証明書は有効か？
S405
N
Y
公開鍵証明書を登録する
S406
END